(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2001 (27.09.2001)

PCT

(10) International Publication Number
WO 01/71462 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/40332

(22) International Filing Date: 20 March 2001 (20.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/531,859 21 March 2000 (21.03.2000) US
09/531,720 21 March 2000 (21.03.2000) US

(71) Applicant: WIDCOMM, INC. [US/US]; Suite 205, 9645 Scranton Road, San Diego, CA 92121 (US).

(72) Inventors: MORRIS, Martin; 1055 Crestview Road, Vista, CA 92083 (US). SENYEI, Andrew; 1574 El Camino del Teatro, La Jolla, CA 92037 (US). CALCAGNO, Jeff; 341 Mesa Way, La Jolla, CA 92037 (US).

(74) Agents: ZIMMER, Kevin, J.; Cooley Godward LLP, 3000 El Camino Real, Five Palo Alto Square, Palo Alto, CA 94306-2155 et al. (US).

(81) Designated States *(national)*: CA, CN, DE, FI, GB, JP, MX, SE.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR SECURE BIOMETRIC IDENTIFICATION

(57) Abstract: A system and method for secure biometric identification. The inventive system includes a mobile unit and a server. The mobile unit is adapted to receive biometric input and provide a first signal in response thereto. In the illustrative implementation, the mobile unit is a Personal Digital Assistant (PDA) and the biometric input is provided by a fingerprint sensor mounted thereon. A first transceiver is mounted on the PDA for transmitting the first signal and receiving a second signal in response thereto. The PDA is adapted to encrypt the first signal and decrypt the second signal. A secure device is mounted at the PDA. The secure device has two modes of operation: a first locked mode by which access thereto is prohibited and a second unlocked mode by which access thereto is enabled on receipt of the second signal. In the illustrative implementation, the secure device is an encrypted database for which the second signal is a decryption key. The server unit includes a second transceiver for receiving the first signal transmitted via the wireless link. The first and second transceivers are adapted to operate in accordance with the Bluetooth specification. The server is equipped with a system for authenticating the biometric data and providing the second signal in response thereto. The second signal is then communicated to the mobile unit where it is utilized to access the secure device, e.g., encrypted database.

WO 01/71462 A2

SYSTEM AND METHOD FOR SECURE BIOMETRIC IDENTIFICATION

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to electronic devices and systems. More specifically, the present invention relates to systems and methods for providing user identification and/or authentication for electronic devices and systems.

Description of the Related Art

Currently, whenever a user wishes to access a computer-based system containing private data, the user must often identify himself, usually with a password. Passwords notoriously provide poor security as users either chose very simple, easily ascertained passwords or, if they use more difficult passwords, users often write them down, making them subject to theft.

In the end, most forms of encryption, as well as access controls such as passwords and even locks, serve a single purpose of identifying the person requesting access.

Hence, there is a need in the art for a reliable, secure system or method of authenticating the identity of a user. Ideally, the system or method would be effective such that one would not need to memorize passwords or utilize other authenticating devices such as keys to access computers and other electronic devices and systems.

SUMMARY OF THE INVENTION

The need in the art is addressed by the system and method for secure biometric identification of the present invention. The inventive system

includes a mobile unit and a server. In the illustrative embodiment, the mobile unit is adapted to receive biometric input and provide a first signal in response thereto. A first transceiver is included for transmitting the first signal and receiving a second signal in response thereto. In an illustrative embodiment, a secure device is operationally coupled to the mobile unit. The secure device has two modes of operation: a first locked mode by which access thereto is prohibited and a second unlocked mode by which access thereto is enabled on receipt of the second signal.

The server unit includes a second transceiver for receiving the first signal transmitted via the wireless link. The server is equipped with a system for authenticating the biometric data and providing the second signal in response thereto. The second signal is then communicated to the mobile unit where it is utilized to access the secure device.

In the illustrative embodiment, the first and second transceivers are adapted to operate in accordance with the Bluetooth specification. Preferably, the mobile unit is adapted to encrypt the first signal and decrypt the second signal. In the illustrative implementation, biometric input is provided by a fingerprint sensor mounted on a Personal Digital Assistant. The secure device in the illustrative implementation is an encrypted database for which the second signal is a decryption key.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1a is a perspective front view of an illustrative implementation of a PDA adapted for use in accordance with the teachings of the present invention.

Fig. 1b is a perspective rear view thereof.

Fig. 2 is a block diagram of an illustrative implementation of a mobile unit subsystem constructed in accordance with the present teachings.

Fig. 3 is a block diagram of an illustrative implementation of a server subsystem for use in the system for secure biometric identification of the present invention.

Fig. 4 is a flow diagram illustrative of a method for secure biometric identification implemented in accordance with the teachings of the present invention.

DESCRIPTION OF THE INVENTION

Illustrative embodiments and exemplary applications will now be described with reference to the accompanying drawings to disclose the advantageous teachings of the present invention.

While the present invention is described herein with reference to illustrative embodiments for particular applications, it should be understood that the invention is not limited thereto. Those having ordinary skill in the art and access to the teachings provided herein will recognize additional modifications, applications, and embodiments within the scope thereof and additional fields in which the present invention would be of significant utility.

As mentioned above, and in accordance with the present teachings, the inventive system includes a mobile unit and a server. In the illustrative embodiment, the mobile unit is a Personal Digital Assistant (PDA) adapted to receive biometric input from a fingerprint sensor and provide a first signal in response thereto. Personal Digital Assistants are well known and widely used.

Fig. 1a is a perspective front view of an illustrative implementation of a PDA adapted for use in accordance with the teachings of the present invention. Fig. 1b is a perspective rear view thereof. In the preferred embodiment, the PDA is implemented in accordance with the teachings of copending U.S. Application No. 09/531,859, filed on March 21, 2000, entitled "SYSTEM AND METHOD FOR SECURE USER IDENTIFICATION WITH BLUETOOTH ENABLED TRANSCEIVER AND BIOMETRIC SENSOR IMPLEMENTED IN A HANDHELD COMPUTER", inventor Martin Morris, (Atty. Docket No. WIDC-011), which teachings are hereby incorporated herein by reference. As disclosed in

the reference application, in the best mode. the PDA 10 is equipped with an expansion slot 12 such as the Visor$_{tm}$ Handheld Computer manufactured and sold by Handspring and disclosed more fully at www.handspring.com. As shown in Fig. 1b, the expansion slot 12 is adapted to receive a card 14 on which a biometric device, in the illustrative embodiment - a fingerprint sensor 16, is disposed. In addition, in accordance with the present teachings, a transceiver 22 is also disposed on the card 14. In the preferred embodiment, the transceiver 22 is adapted to operate in accordance with the BLUETOOTH SPECIFICATION VERSION 1.0A CORE, published in July 1999. When the card is inserted into the expansion slot, it interfaces electrically with the system bus of the PDA and provides an electrical circuit depicted in Fig. 2.

Fig. 2 is a block diagram of an illustrative implementation of a mobile unit subsystem constructed in accordance with the present teachings. The mobile unit subsystem 20 includes the wireless transceiver 22 which is adapted to communicate with a central processing unit (CPU) 26 of the PDA. The central processing unit 26 receives biometric data from the fingerprint sensor 28. In accordance with the present teachings, data from the fingerprint sensor 28 is encrypted in either in software 30 adapted to run on the CPU 26 and/or in optional hardware 32. Encryption hardware and software are well known in the art. The control software 30 also enables the CPU 26 to selectively access and control the mobile unit components via a system bus shown generally at 38.

The encrypted biometric data is either used locally to access an encrypted database 34 or, preferably, transmitted over a link such as a wireless link to a server subsystem via the transceiver 22 and antenna 24. The server subsystem is depicted in Fig. 3.

Fig. 3 is a block diagram of an illustrative implementation of a server subsystem for use in the system for secure biometric identification of the present invention. The encrypted biometric data signal is received by a server antenna 42 and a second wireless Bluetooth enabled transceiver 44. The received signal is decrypted by an optional conventional hardware

based decryption circuit 46 and/or by decryption software implemented in control software 48 adapted to run on a server CPU 50. Those skilled in the art will appreciate that the decryption scheme utilized on the server is designed to match that of the mobile unit 20. In the preferred embodiment, the RSA public key encryption scheme is used. This scheme is disclosed more fully in U.S. Patent No. 4,405,829 entitled Cryptograpgic Communications System & Method, issued 9/29/83 to Rivest, et al. the teachings of which are incorporated herein by reference. The server control software also controls the CPU 50 to selectively access and control the components of the server subsystem 40 via a server subsystem bus shown generally at 51.

In accordance with the present teachings, the decrypted biometric data, in the illustrative implementation, the decrypted fingerprint, is compared by fingerprint matching software 52 to a database 54 of biometric data, i.e., fingerprints. Fingerprint matching software is well known in the art. Such software may be purchased from Veridicom, Inc. of Santa Clara, CA.

When a match is achieved, a user is identified and an authentication key specific to the identified mobile user is retrieved from an encryption key database by the CPU 50 via the bus 51. In the preferred embodiment, the retrieved encryption key is encrypted by the resident encryption scheme either by the hardware unit 46, if provided, and/or by the encryption software implemented in the control software 48. The encrypted encryption key is then transmitted back to the mobile unit 20 via the wireless link through the transceiver 44 and antenna 42. As an alternative, the encrypted encryption key may be provided to a network 59 via a first network interface card or circuit 58 and a second network interface card or circuit 66. The network 59 facilitates the communication of the encrypted encryption key to the mobile unit 20 via a wireless transceiver 62 and an antenna 64. This configuration may be preferred if the second antenna 64 is closer to the mobile unit 20.

In addition, those skilled in the art will appreciate that the inventive system can be implemented such that the encrypted biometric data is transmitted from a first PDA 20 and the encrypted encryption key or other information is sent to a second mobile unit or over a network to a second server or network of devices.

Returning to Fig. 2, on receipt of the encrypted encryption key from the server subsystem 40 via the antenna 24 and the wireless transceiver 22, the mobile unit CPU 26 decrypts the encrypted key using the resident software and/or hardware decryption facility 30 and 32, respectively. The decrypted encryption key is then used by the CPU 26 to access a secure device. In an illustrative embodiment, the secure device is an encrypted database 34 mounted on the mobile unit. Those skilled in the art will appreciate that the secure device need not be mounted on the mobile unit 20. As an alternative, the secure device may be coupled to the mobile unit via the wireless link.

In any event, the secure device, i.e., database 34, has two modes of operation: a first locked mode by which access thereto is prohibited and a second unlocked mode by which access thereto is enabled on receipt of the decrypted encryption key. For optimal security, the decryption key for the encrypted database 34 should not be stored on the mobile unit. On receipt of the decrypted decryption key, a working copy 36 of the encrypted database 34 is created.

Fig. 4 is a flow diagram illustrative of a method for secure biometric identification implemented in accordance with the teachings of the present invention. As shown in Figs. 2, 3 and 4 when a user in possession of the mobile unit 20 wishes to access the secure device 34, he/she places a finger on the fingerprint sensor 28 and starts the access control program 100.

At step 104, the CPU 26 running the access control software 30 scans the fingerprint from sensor 28 and, at step 106, encrypts it with the public key of the authentication server 40 by using the encryption software or hardware 30, 32.

At step 108, the resulting encrypted message is sent to the server 40 via the transceiver 22 and antenna 24 on the mobile unit 20 and the antenna 42 and transceiver 44 of the server 40. As mentioned above, as an alternative, the encrypted fingerprint is sent via the access point 60 and local or wide-area network 59 when the server 40 is not within direct radio range of the mobile unit 20.

At step 110, when the authentication request is received at the server 40, the server CPU 50 decrypts the message using its secret key and the encryption hardware and/or software 46 and 48, respectively.

At step 112, the CPU 50 then utilizes the fingerprint match software 52 to compare the decrypted fingerprint to the database of authorized fingerprints 54 to determine if the request is valid.

If the request is valid, then, at step 114, the decryption key for the user's encrypted database 34 (Fig. 2) is retrieved from the key database 56 (Fig. 3).

At step 116, the key is encrypted via the encryption hardware or software 46, 48 (Fig. 3) and, at step 118, sent back to the mobile unit 20 via the same path from which the request was originally received.

At the mobile unit 20, at steps 122 and 124, the key is received and decrypted.

At step 126, the retrieved key used to make a temporary working copy 36 of the encrypted database 34.

At step 128 this temporary copy 36 is either read or edited.

If edited, then at step 130 the edited working copy is deleted or rewritten to encrypted form as soon as the user completes his operation.

Thus, the present invention has been described herein with reference to a particular embodiment for a particular application. Those having ordinary skill in the art and access to the present teachings will recognize additional modifications applications and embodiments within the scope thereof.

It is therefore intended by the appended claims to cover any and all such applications, modifications and embodiments within the scope of the present invention.

Accordingly,

WHAT IS CLAIMED IS:

1. A system for secure biometric identification comprising:

first means for receiving biometric input and providing a first signal in response thereto;

second means for transmitting said first signal and receiving a second signal in response thereto; and

third means operationally coupled to said second means for disabling access to a resource in a first locked mode of operation and enabling access to said resource in a second unlocked mode of operation on receipt of said second signal.

2. The invention of Claim 1 further including means for encrypting said first signal.

3. The invention of Claim 1 wherein said first means is a fingerprint sensor.

4. The invention of Claim 1 further including means for decrypting said second signal.

5. The invention of Claim 1 wherein said second means is a wireless transceiver.

6. The invention of Claim 5 wherein said second means is a transceiver adapted to operate in accordance with a Bluetooth specification.

7. The invention of Claim 1 wherein said third means is a database.

8. The invention of Claim 7 wherein said database is encrypted and said second signal is a key for decrypting same to provide a decrypted database.

9. The invention of Claim 8 further including means for providing a working copy of said decrypted database.

10. The invention of Claim 1 further including a processor connected to said first, second and third means.

11. The invention of Claim 10 wherein said processing unit is a central processing unit.

12. The invention of Claim 11 further including software for controlling said central processing unit to sequentially activate said first, second and third means.

13. A mobile unit for use in a system for secure biometric identification comprising:

a biometric sensor;

a central processing unit coupled to said biometric sensor;

software running on said central processing unit;

a transceiver coupled to said sensor; and

a device coupled to said transceiver, said device having two modes of operation, a first locked mode by which access thereto is prohibited and a second unlocked mode by which access thereto is enabled on receipt of a signal from said transceiver.

14. A server unit for use in a system for secure biometric identification comprising:

first means for receiving biometric data via a wireless link;

second means for authenticating said biometric data and providing a signal in response thereto; and

third means for transmitting said signal via said wireless link.

15. The invention of Claim 14 wherein said first means includes means for decrypting said biometric data.

16. The invention of Claim 14 wherein said second means includes a processor.

17. The invention of Claim 16 wherein said processor is a central processing unit.

18. The invention of Claim 17 wherein said second means includes a database of biometric data.

19. The invention of Claim 18 wherein said second means includes software adapted to run on said processor and match said received biometric data with biometric data stored in said database.

20. The invention of Claim 19 wherein said second means further includes a database of encryption keys.

21. The invention of Claim 20 wherein said second means outputs said signal on identification of a match of said received biometric to biometric data stored in said database by said processor.

22. The invention of Claim 21 wherein said signal is a key from said database of encryption keys.

23. The invention of Claim 16 wherein said first and said third means is a wireless transceiver.

24. The invention of Claim 23 wherein said wireless transceiver operates in accordance with a Bluetooth specification.

25. A system for secure biometric identification comprising:

first means receiving biometric input and providing a first set of biometric data in response thereto;

second means for transmitting a first signal representative of said biometric data;

third means for receiving said first signal and providing a second signal in response thereto;

fourth means for authenticating said second signal and providing a third signal in response thereto; and

fifth means for providing an fourth signal in response to said third signal.

26. The invention of Claim 25 wherein said first means includes a fingerprint sensor.

27. The invention of Claim 25 wherein said first means includes means for encrypting said biometric data.

28. The invention of Claim 25 wherein said second means is a wireless transmitter.

29. The invention of Claim 28 wherein said second means is a transceiver.

30. The invention of Claim 29 wherein said second means is a transceiver adapted to operate in accordance with a Bluetooth specification.

31. The invention of Claim 25 wherein said third means is a wireless receiver.

32. The invention of Claim 31 wherein said third means is a transceiver.

33. The invention of Claim 32 wherein said third means is a transceiver adapted to operate in accordance with a Bluetooth specification.

34. The invention of Claim 25 wherein said third means includes means for decrypting said first signal to provide said second signal.

35. The invention of Claim 25 wherein said fourth means includes means for comparing said second signal to at least one stored signal.

36. The invention of Claim 35 wherein said fourth means includes a processor.

37. The invention of Claim 36 wherein said fourth means includes means for storing a second set of biometric data.

38. The invention of Claim 37 further including means for controlling said processor to compare said first set of biometric data to said second set of biometric data.

39. The invention of Claim 38 wherein said means for controlling includes biometric matching software.

40. The invention of Claim 39 wherein said biometric matching software is fingerprint matching software.

41. The invention of Claim 25 wherein said fifth means is a decryption key.

42. The invention of Claim 41 wherein said fourth signal includes a public decryption key.

43. The invention of Claim 42 further including a secure device in communication with said second means.

44. The invention of Claim 43 wherein said secure device is responsive to said decryption key.

45. The invention of Claim 25 wherein said first and second means are mounted on a Personal Digital Assistant.

46. A system for secure biometric identification comprising:

a handheld computer enabled device;

a fingerprint sensor mounted on said device for providing a first set of biometric data;

means disposed on said device for encrypting said biometric data;

a first wireless transceiver mounted on said device for transmitting a first signal representative of said biometric data;

a second wireless transceiver for receiving said first signal and providing a second signal in response thereto;

means for decrypting said second signal to provide said first set of biometric data;

means for authenticating said first set of biometric data and providing a third signal in response thereto, said means for authenticating including means for comparing said first set of biometric data to plural second sets of biometric data;

means for providing a decryption key to said second means in response to said third signal; and

a secure device in communication with said second means and responsive to said decryption key.

47. The invention of Claim 46 wherein said first transceiver is a transceiver adapted to operate in accordance with a Bluetooth specification.

48. The invention of Claim 46 wherein said second transceiver is a transceiver adapted to operate in accordance with a Bluetooth specification.

49. The invention of Claim 46 wherein said means for comparing includes biometric matching software.

50. The invention of Claim 49 wherein said biometric matching software is fingerprint matching software.

51. The invention of Claim 46 wherein decryption key is a public decryption key.

52. The invention of Claim 46 wherein said handheld device is a Personal Digital Assistant.

53. A system for secure biometric identification comprising:

a computer enabled device;

a biometric sensor mounted on said device;

a first central processing unit in communication with said sensor;

a first wireless transceiver mounted on said device and coupled to said first central processing unit;

a second wireless transceiver in communication with said first wireless transceiver;

a second central processing unit in communication with said second transceiver;

software running on said second central processing unit for authenticating a signal transmitted by said first transceiver and received by said second transceiver and providing a decryption key in response thereto;

a secure device mounted on said computer enable device and responsive to said decryption key.

54. The invention of Claim 53 wherein said first transceiver is a transceiver adapted to operate in accordance with a Bluetooth specification.

55. The invention of Claim 53 wherein said second transceiver is a transceiver adapted to operate in accordance with a Bluetooth specification.

56. The invention of Claim 53 wherein decryption key is a public decryption key.

57. The invention of Claim 53 wherein said handheld device is a Personal Digital Assistant.

58. A method for secure biometric identification including the steps of:

providing biometric data from a first unit;

transmitting a first signal from said first unit representative of said biometric data via a wireless link;

receiving said first signal at a second unit; and

authenticating said first signal at said second unit and transmitting a second signal in response thereto via said wireless link.

59. The invention of Claim 58 further including the step of using said second signal to access a secure resource.

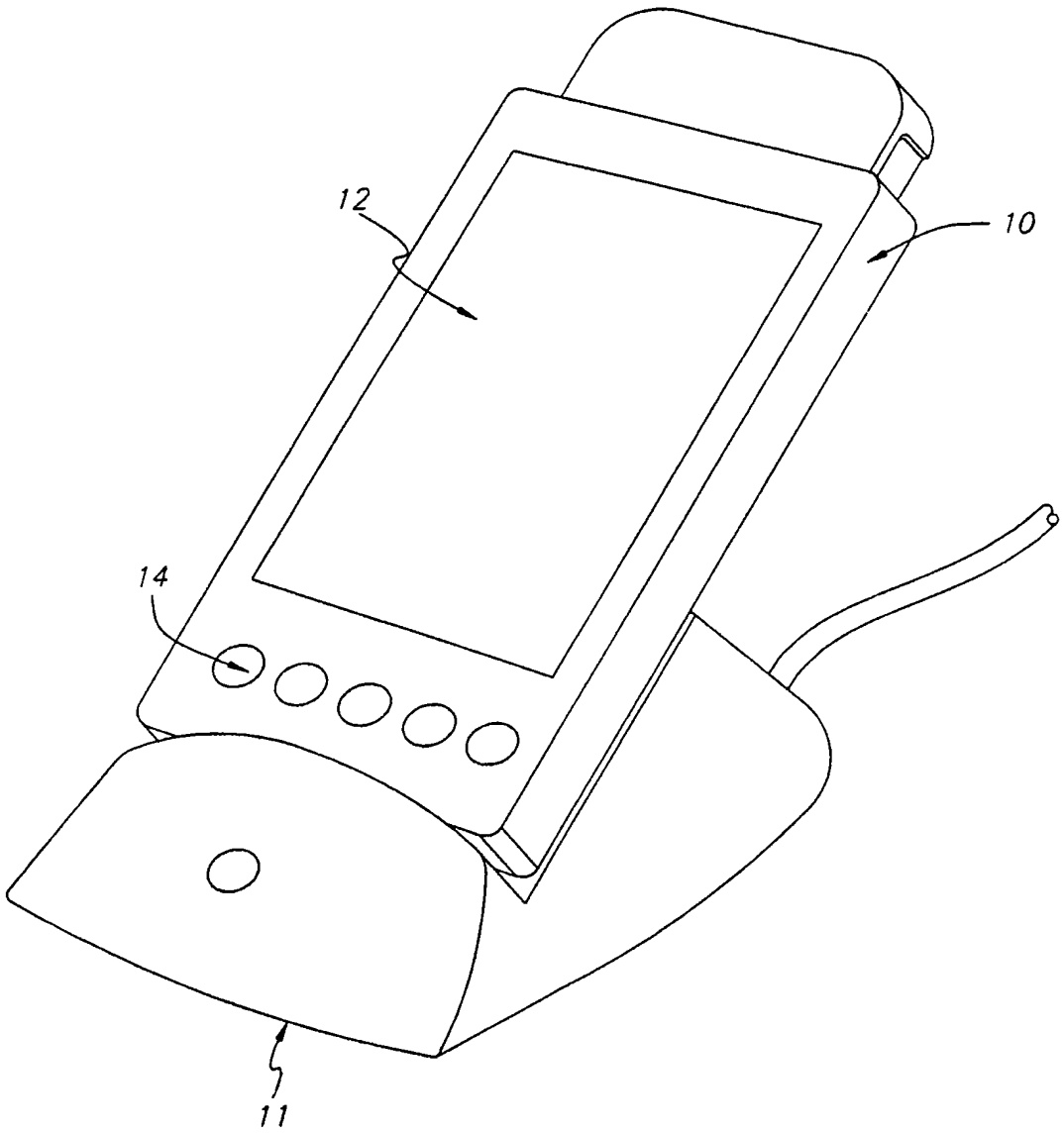

FIG. 1(a)

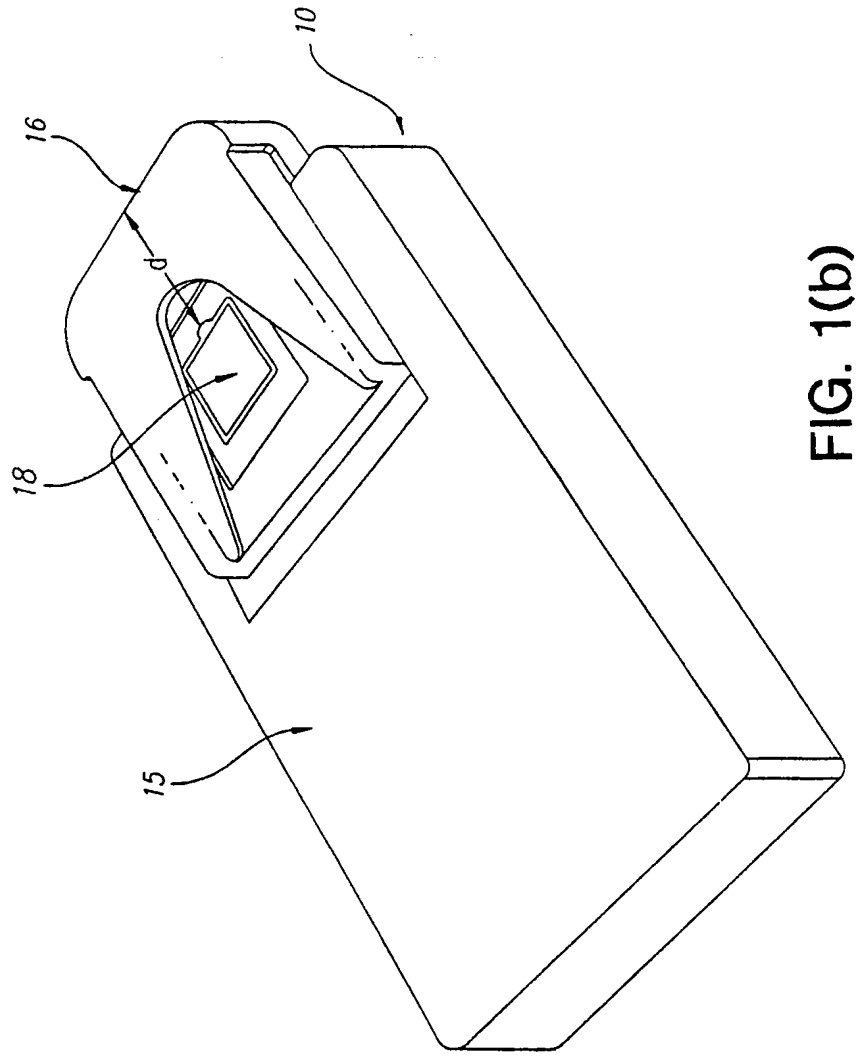

FIG. 1(b)

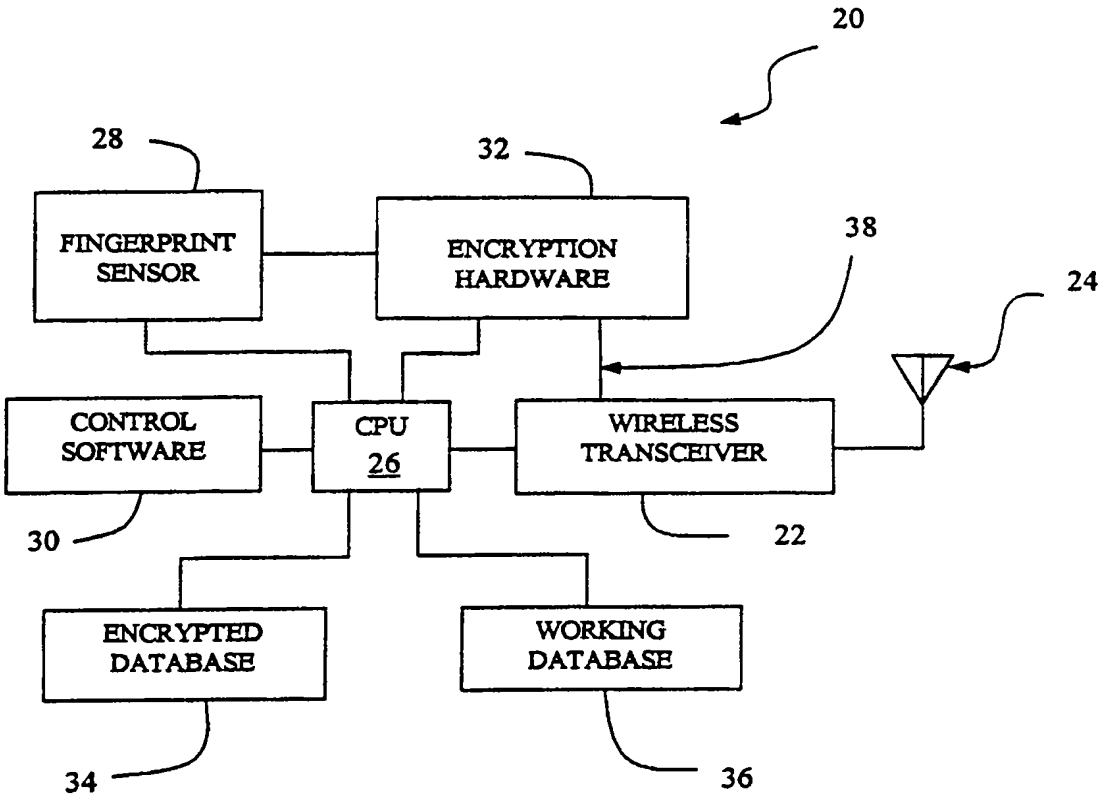
20
28
32
FINGERPRINT SENSOR
ENCRYPTION HARDWARE
38
24
CONTROL SOFTWARE
CPU 26
WIRELESS TRANSCEIVER
30
22
ENCRYPTED DATABASE
WORKING DATABASE
34
36

FIG. 2

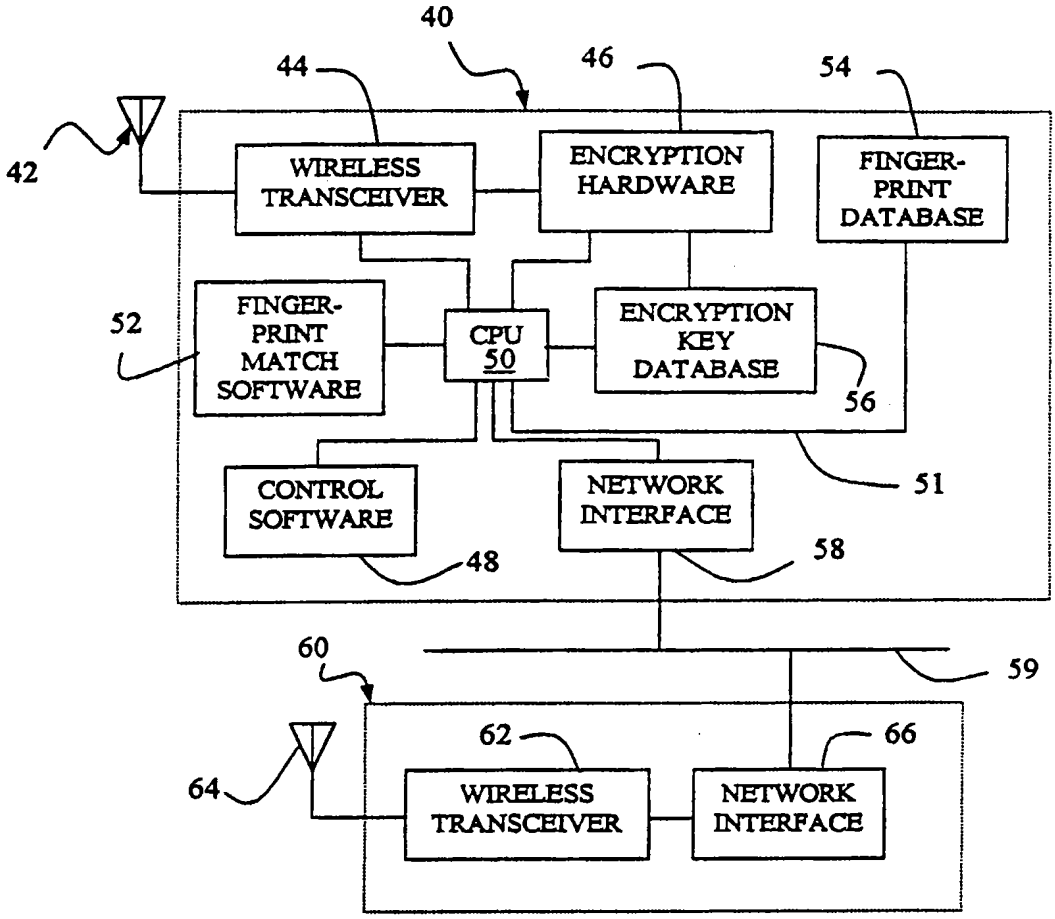
40
44
46
54
42
WIRELESS TRANSCEIVER
ENCRYPTION HARDWARE
FINGER-PRINT DATABASE
52
FINGER-PRINT MATCH SOFTWARE
CPU 50
ENCRYPTION KEY DATABASE
56
51
CONTROL SOFTWARE
NETWORK INTERFACE
48
58
60
59
62
66
64
WIRELESS TRANSCEIVER
NETWORK INTERFACE

FIG. 3

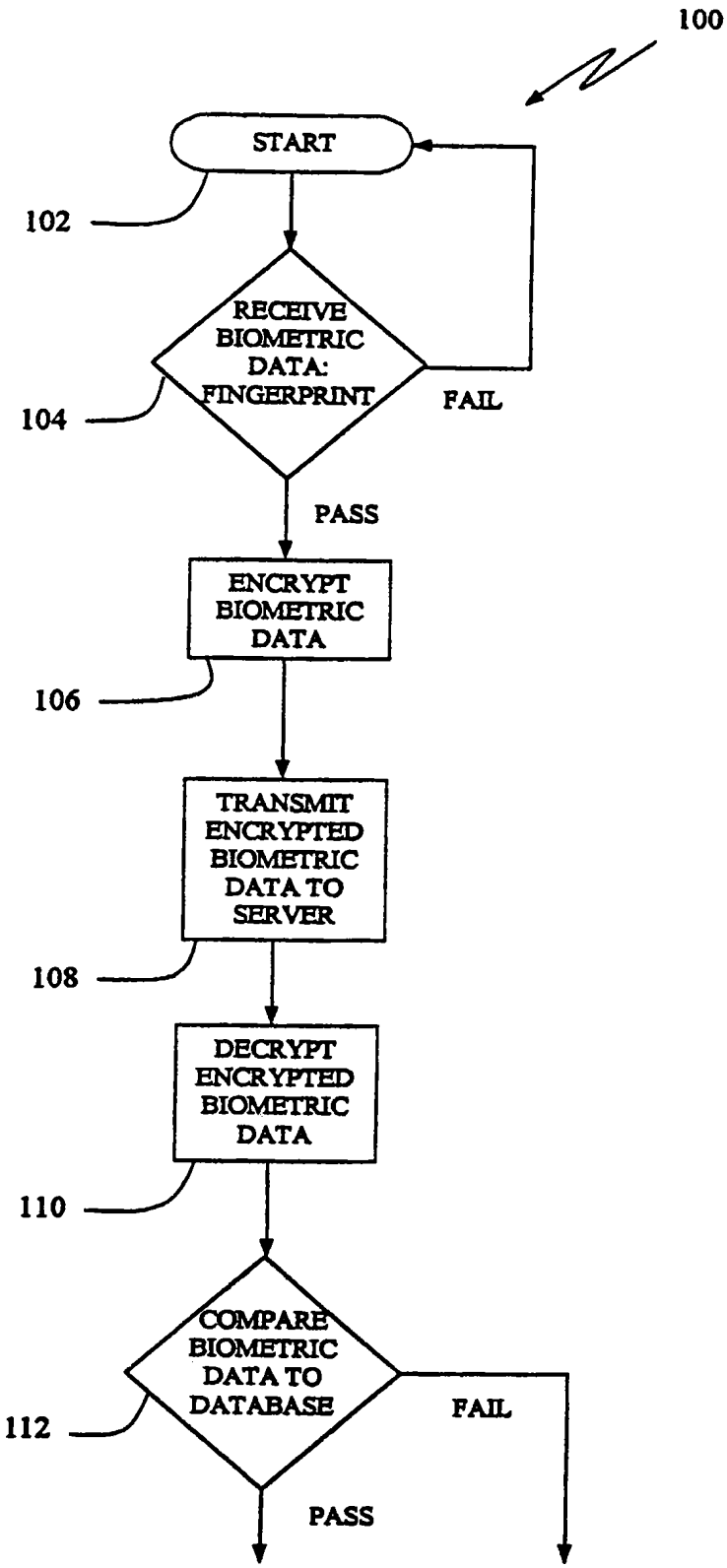
100
START
102
RECEIVE BIOMETRIC DATA: FINGERPRINT
104
FAIL
PASS
ENCRYPT BIOMETRIC DATA
106
TRANSMIT ENCRYPTED BIOMETRIC DATA TO SERVER
108
DECRYPT ENCRYPTED BIOMETRIC DATA
110
COMPARE BIOMETRIC DATA TO DATABASE
112
FAIL
PASS

FIG. 4(a)

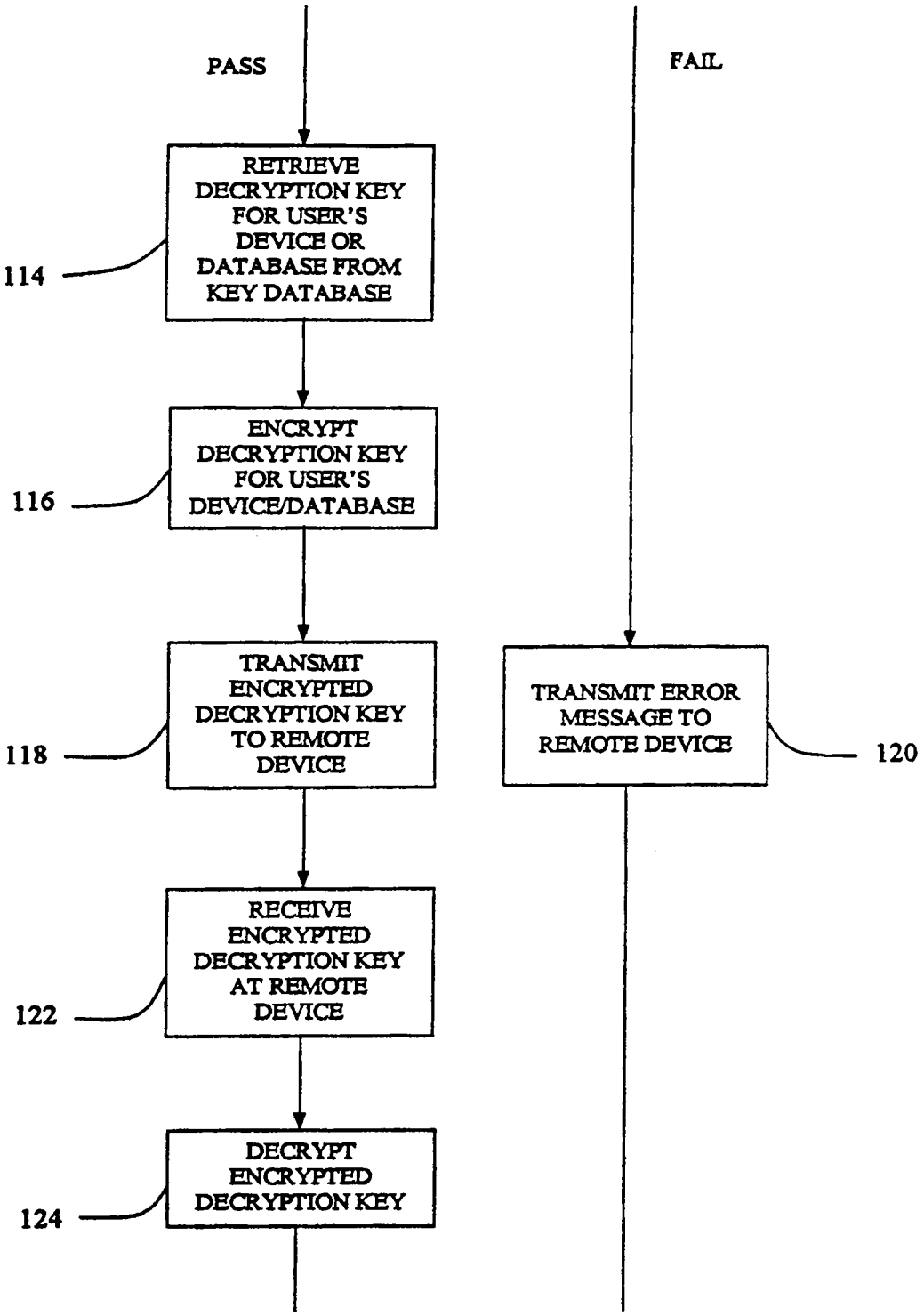
PASS
FAIL
RETRIEVE DECRYPTION KEY FOR USER'S DEVICE OR DATABASE FROM KEY DATABASE
114
ENCRYPT DECRYPTION KEY FOR USER'S DEVICE/DATABASE
116
TRANSMIT ENCRYPTED DECRYPTION KEY TO REMOTE DEVICE
118
TRANSMIT ERROR MESSAGE TO REMOTE DEVICE
120
RECEIVE ENCRYPTED DECRYPTION KEY AT REMOTE DEVICE
122
DECRYPT ENCRYPTED DECRYPTION KEY
124

FIG. 4(b)

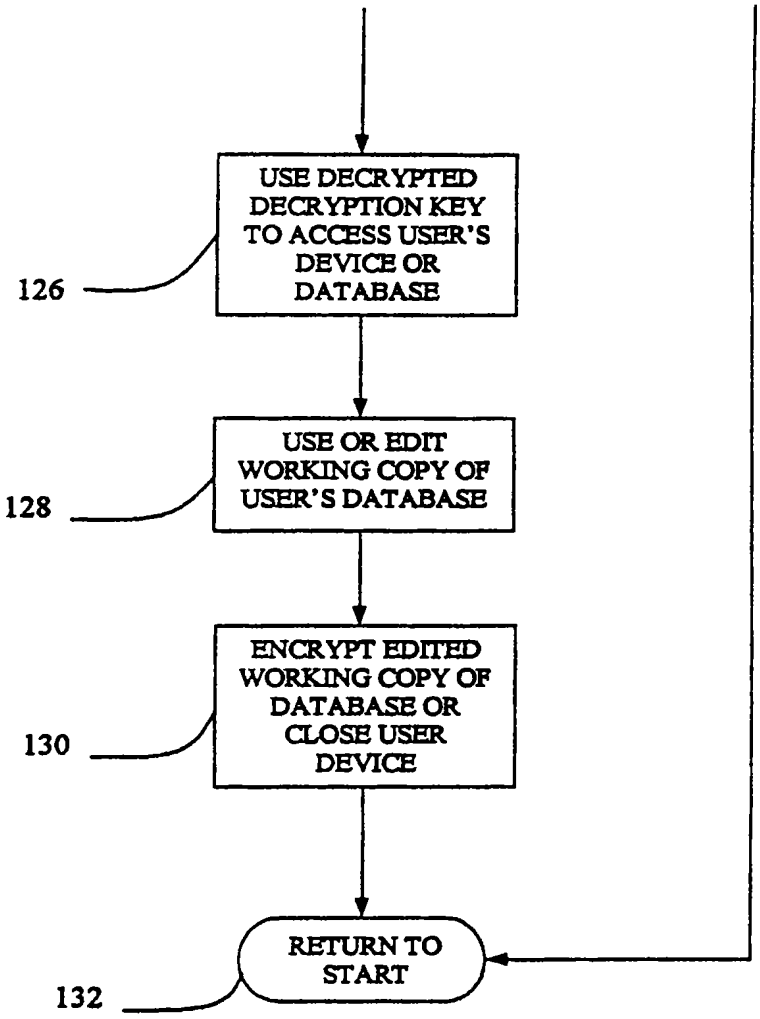
USE DECRYPTED DECRYPTION KEY TO ACCESS USER'S DEVICE OR DATABASE
126
USE OR EDIT WORKING COPY OF USER'S DATABASE
128
ENCRYPT EDITED WORKING COPY OF DATABASE OR CLOSE USER DEVICE
130
RETURN TO START
132

FIG. 4(c)